

D R A F T

6 May 1981

PROPOSED CHANGES TO DCID 1/14
RECOMMENDED BY THE
INVESTIGATIVE STANDARDS WORKING GROUP

DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE NO. 1/14¹

MINIMUM PERSONNEL SECURITY STANDARDS AND PROCEDURES
GOVERNING ELIGIBILITY FOR ACCESS TO SENSITIVE
COMPARTMENTED INFORMATION

(Effective _____ 1981)

Pursuant to the provisions of Executive Order 11905 12036, Section 102 of the National Security Act of 1947 and National Security Council Directives, the following minimum personnel security standards, procedures and continuing security programs are hereby established for all United States Government civilian and military personnel, consultants, contractors, employees of contractors and other individuals who require access to Sensitive Compartmented Information² (hereinafter referred to as SCI). The standards, procedures and programs established herein are minimum and the departments and agencies may establish such additional security steps as may be deemed necessary and appropriate to ensure that effective security is maintained.

Purpose

1. The purpose of this Directive is to enhance the security protection of SCI through the application of minimum security standards, procedures and continuing security programs, and to facilitate the security certification process among Government departments and agencies.

Applicability

2. The provisions of the Directive shall apply to all persons (other than elected officials of the United States Government, federal judges and those individuals for whom the DCI makes a specific exception) without regard to civilian or military status, form of employment, official rank or position or length of service.

3. Individuals who do not meet the minimum security criteria contained herein and who are, therefore, denied access to SCI shall not, solely, for this reason, be considered ineligible for access to other classified information. Individuals whose access to SCI has been authorized as an exception granted in accordance with paragraph 76 below, shall not, solely for that reason, be considered eligible for access to other classified information.

¹This directive supersedes DCID 1/14 approved 13 May 1976.

²The term "Sensitive Compartmented Information" as used in this Directive is intended to include all information and materials bearing special community controls indicating restricted handling within present and future community intelligence collection programs and their end products for which community systems of compartmentation have been or will be formally established. The term does not include Restricted Data as defined in Section II, Public Laws 585, Atomic Energy Act of 1954, as amended.

General

4. The granting of access to SCI shall be controlled under the strictest application of the "need-to-know" principle under procedures prescribed in the several existing authorities which govern access thereto, and in accordance with the personnel security standards and procedures set forth in this Directive.

A TOP SECRET security clearance is a prerequisite for nominees for SCI access.

All persons accountable under the authority of this Directive and given access to information (SCI) containing sources or methods of intelligence shall, as a condition of obtaining access, sign an agreement that they will not disclose that information to persons not authorized to receive it.

Personnel Security Standards

5. Criteria for security approval of an individual on a need-to-know basis for access to SCI are as follows:

a. The individual shall be stable, of excellent character and discretion and of unquestioned loyalty to the United States.

b. Except where there is a compelling need, and a determination has been made by competent authority as described in paragraph 7 below that every reasonable assurance has been obtained that under the circumstances the security risk is negligible:

(1) Both the individual and the members of his or her immediate family shall be U.S. citizens. For these purposes, "immediate family" is defined as including includes the individual's spouse or cohabitant, parents, brothers, sisters and children.

(2) The members of the individual's immediate family and persons to whom he is bound by affection or obligation should neither be subject to physical, mental or other forms of duress by a foreign power, nor advocate the use of force or violence to overthrow the Government of the United States or the alteration of the form of Government of the United States by unconstitutional means.

Exceptions

7: 6. The exceptions to paragraph 5.b.(1)(2) above may be granted only by the Senior Intelligence Officer (SIO) of the Intelligence Community organization or his designee unless such authority has been specifically delegated to the head of an

office or organization as set forth in inter-departmental agreements. All exceptions granted will be common sense determinations based on all available information, and shall be recorded by the agency making the exception. In those cases in which the individual has lived outside of the United States for a substantial period of his life, a thorough assessment of the adequacy of the investigation in terms of fulfillment of the minimum investigative requirements, and judicious review of the information therein must be made before an exception is considered.

Investigative Requirements

7 8. The investigation conducted on an individual under consideration for access to SCI will be thorough and shall be designed to develop information as to whether the individual clearly meets the above Personnel Security Standards.

3 9. The investigation shall be accomplished through record checks and personal interviews of various sources by trained investigative personnel in order to establish affirmatively to the adjudicating agency complete continuity of identity to include birth, residences, education, employments and military service. Where the circumstances of a case indicate, the investigation shall exceed the basic requirements set out below to ensure that those responsible for adjudicating access eligibility have in their possession all the relevant facts available.

7 10. The individual shall furnish a signed personal history statement, fingerprints of a quality acceptable to the Federal Bureau of Investigation and a signed release, as necessary, authorizing custodians of police, credit, education and medical records, to provide record information to the investigative agency. Photographs of the individual shall also be obtained where additional corroboration of identity is required.

11. Minimum standards for the investigation are as follows.

a. Verification of date and place of birth and citizenship.

b. Check of the subversive and criminal files of the Federal Bureau of Investigation, including submission of fingerprint charts, and such other National agencies as are appropriate to the individual's background. An additional check of Immigration and Naturalization Service records shall be conducted on those members of the individual's immediate family who are United States citizens other than by birth or who are resident aliens.

c. A check of appropriate police records covering all areas where the individual has resided in the US throughout the most recent fifteen (15) years or since age eighteen, whichever is the shorter period.

d. Verification of the individual's financial status and credit habits through checks of appropriate credit institutions and interviews with knowledgeable sources covering the most recent five (5) years.

e. Interviews with neighbors in the vicinity of all the individual's residences in excess of six (6) months throughout the most recent five (5) year period. This coverage shall be expanded where the investigation suggests the existence of some questionable behavioral pattern.

f. Confirmation of all employment during the past fifteen (15) years or since age eighteen, whichever is the shorter period but in any event the most recent two years. Personal interviews with supervisors and co-workers at places of employment covering the past ten (10) years shall be accomplished.

g. Verification of attendance at institutes of higher learning in all instances and at the last secondary school attended within the past fifteen (15) years. Attendance at secondary schools may be verified through qualified collateral sources. If attendance at educational institutions occurred within the most recent five (5) years, personal interviews with faculty members or other persons who were acquainted with the individual during his attendance shall be accomplished.

h. Review of appropriate military records.

i. Interviews with a sufficient number of knowledgeable acquaintances (a minimum of three developed during the course of the investigation) as necessary to provide a continuity to the extent practicable, of the individual's activities and behavioral patterns over the past fifteen years with particular emphasis on the most recent five years.

j. When employment, education or residence has occurred overseas (except for periods of less than five (5) years one year for personnel on US Government assignment and less than ninety days for other purposes) during the past fifteen years or since age eighteen, a check of the records will be made at the Department of State and / or other appropriate agencies. Efforts shall be made to develop sources, generally in the United States, who knew the individual overseas in order to cover significant employment, education or residence and to attempt to determine if any lasting foreign contacts or connections were established during this period. However, in all cases where an individual has worked or lived outside of the US continuously for over five years one year, the investigation will be expanded to cover fully this period in his life through the use of such investigative assets and checks of record sources as may be available to the US Government in the foreign country(ies) in which the individual resided.

k. In these instances in which When the individual has immediate family members or other persons with to whom he the individual is bound by affection or obligation in any of the situations described in subparagraph 5.b.(2), above, the investigation will include an interview of the individual by trained security, investigative or counter-intelligence personnel to ascertain the facts as they may relate to the individual's access eligibility.

1. In all cases, the individual's spouse or cohabitant shall at a minimum be checked through the subversive and criminal files of the Federal Bureau of Investigation and other National agencies as appropriate. When conditions indicate, additional investigation shall be conducted on the spouse of the individual and members of the immediate family (or other persons to whom the individual is bound by affection or obligation) to the extent necessary to permit a determination by the adjudicating agency that the provisions of paragraph 5 (Personnel Security Standards) above are met (See Annex A).

m. A personal interview of the individual will be conducted by trained security, investigative or counter-intelligence personnel when necessary to resolve any significant adverse information and/or inconsistencies developed during the investigation.

n. All nominees for access to SCI shall be interviewed by trained security personnel utilizing the polygraph (see Annex C).

11. (Old Paragraph 6) In exceptional cases, the Senior Intelligence Officer (SIO) of the Intelligence Community organization; The SIO or his designee may determine that it is necessary or advisable in the National interest to authorize access to SCI prior to completion of the fully prescribed investigation noted in paragraph 10 above.

In this situation, such investigative checks as are immediately possible shall be made at once and should shall include a personal interview by trained security personnel utilizing the polygraph (see Annex C). Access in such cases shall be strictly controlled, and the fully prescribed investigation and final evaluation shall be completed at the earliest practicable moment.

12. Where a previous investigation has been conducted within the past five years which substantially meets the above minimum standards, it may serve as a basis for granting access approval provided a polygraph examination together with a review of the personnel and security files does do not reveal substantive changes in the individual's security eligibility. If a previous investigation does not substantially meet the minimum standards or if it is more than five years old, a current investigation shall be required but may be limited to a polygraph examination and whatever else is necessary to bring the individual's file up-to-date in accordance with the other investigative requirements set forth in paragraph 10 above.

Should new information be developed during the current investigation which bears unfavorably upon the individual's activities covered by the previous investigation, the current inquiries shall be expanded as necessary to develop full details of this new information.

13. Programs shall be instituted requiring the periodic reinvestigation of personnel provided access to SCI. These reinvestigations will be conducted on a five year recurrent basis, but on a more frequent basis where the individual has shown some questionable behavioral pattern, his activities are otherwise suspect, or when deemed necessary by the SIO concerned.³

14. The scope of reinvestigations shall be determined by the SIO concerned based on such considerations as the potential damage that might result from the individual's defection or willful compromise of SCI and the availability and probable effectiveness of other means to continually evaluate factors related to the individual's suitability for continued access. In all cases, the reinvestigation shall include, as a minimum, ~~appropriate National agency checks, local agency (including overseas checks where appropriate), credit checks and a personal discussion with the individual by trained investigative, security or counterintelligence personnel when necessary to resolve significant adverse information or inconsistencies.~~

a personal interview with the individual by trained security personnel utilizing the polygraph (see Annex C).
The individual shall furnish an up-to-date, signed personal history statement and signed releases, as appropriate. When conditions indicate, additional investigation may be conducted as determined by the SIO.

15. The evaluation of the information developed by investigation on an individual's loyalty and suitability shall be accomplished under the cognizance of the SIO concerned by analysts of broad knowledge, good judgment and wide experience in personnel security and/or counterintelligence. When all other information developed on an individual is favorable, a minor investigative requirement which has not been met should not preclude favorable adjudication. In all evaluations the protection of the national interest is paramount. Any doubt concerning personnel having access to SCI shall be resolved in favor of the national security. The ultimate determination of whether the granting of access is clearly consistent with the interest of national security shall be an overall common sense determination based on all available information.

³ In DoD, an SIO may request, with the approval of the Secretary of Defense or his designee, more frequent reinvestigations under special circumstances.

Continuing Security Programs

16. In order to facilitate the attainment of the highest standard of personnel security and to augment both the access approval criteria and the ~~investigate~~ investigative

requirements established by this Directive, member departments and agencies shall institute continuing security programs for all individuals having access to SCI. In addition to security indoctrinations

(See Annex D, "Minimum Standards for Security Awareness Programs in the U.S. Intelligence Community"),

, these programs shall be tailored to create mutually supporting procedures under which no issue will escape notice or be left unresolved which brings into question an individual's loyalty and integrity or suggests the possibility of his being subject to undue influence or duress through foreign

relationships or exploitable personal conduct. When an individual is assigned to perform sensitive compartmented work requiring access to SCI, the SIO for the department, agency or Government program to which the individual is assigned shall assume security supervision of that individual throughout the period of his assignment.

17. The continuing security programs shall include the following:

a. Security education programs ~~to ensure that individuals who are granted access to SCI are initially indoctrinated and periodically thereafter instructed as to its unique sensitivity and that they understand their personal responsibility for maintaining eligibility for continued access to SCI rests with the individual.~~

of the member departments and agencies shall be established and maintained pursuant to the requirements of Annex D. Additionally, Therefore,

the individual is encouraged to seek appropriate guidance and assistance on any personal problem or situation which may have a possible bearing on his eligibility for continued access to SCI, and security counseling should be made available. These instructions should be conducted by individuals having extensive background and experience regarding the nature and special vulnerabilities of the particular type of compartmented information involved.

b. Security supervisory programs to ensure that supervisory personnel recognize and discharge their special responsibility in matters pertaining to the security of SCI, including the eligibility for SCI access. Such programs shall provide practical guidance as to indicators which may signal matters of security concern. Specific instructions concerning reporting procedures shall be disseminated to enable the appropriate authority to take timely corrective action to safeguard the security of the United States as well as to provide all necessary help to the individual concerned to neutralize his vulnerability.

c. Security Review Programs to ensure that appropriate security authorities invariably receive and exchange, in a timely manner, all information bearing on the security posture of persons having access to sensitive information. Personnel history information shall be kept current. Security and related files shall be kept under continuing review.

18. Whenever adverse or derogatory information is discovered or inconsistencies arise which could impact upon an individual's security status, appropriate investigations shall be conducted on a timely basis. The investigation shall be of sufficient scope necessary to resolve the specific adverse or derogatory information, or inconsistency, in question so that a determination can be made as to whether the individual's continued utilization in activities requiring SCI is clearly consistent with the interests of the national security.

Effective Date

13 May 1976.

19. This Directive supersedes DCID 1/14, ~~1 July 1968~~. Existing directives,* regulations, agreements and such other references governing access to SCI as defined herein shall be revised accordingly.

* These include pertinent provisions of the Clearance Standards and Investigation and Evaluation section of the Communications Intelligence Security Regulations.

WILLIAM J. CASEY

~~GEORGE BUSH~~

Director of Central Intelligence

19 March 1980

ANNEX A

DCID 1/14 ADJUDICATION GUIDELINES

PURPOSE

This annex is designed to ensure that a common approach is followed by Intelligence Community Departments and Agencies in applying the standards of DCID 1/14. These guidelines apply to the adjudication of cases involving persons being considered for first time access to Sensitive Compartmented Information (SCI) as well as those cases of persons being readjudicated for continued SCI access.

ADJUDICATIVE PROCESS

The adjudicative process entails the examination of a sufficient period of a person's life to make a determination that the person is not now or is not likely to later become an unacceptable security risk. SCI access adjudication is the careful weighing of a number of variables known as the "whole person" concept. The recency of occurrence of any adverse incident, together with circumstances pertaining thereto, is central to a fair and uniform evaluation. Key factors to be considered in adjudication are the maturity and responsibility of the person at the time certain acts or violations were committed as well as any repetition or continuation of such conduct. Each case must be judged on its own merits and final determination remains the responsibility of the individual SIO. Any doubt concerning personnel having access to SCI shall be resolved in favor of the national security.

The ultimate determination of whether the granting of SCI access is clearly consistent with the interests of national security shall be an overall common sense determination based on all available information. In arriving at a decision consistent with the foregoing, the adjudicator must give careful scrutiny to the following matters:

- a. Loyalty
- b. Close relatives and associates
- c. Homosexual conduct and sexual perversion
- d. Cohabitation
- e. Undesirable character traits
- f. Financial irresponsibility
- g. Alcohol abuse
- h. Illegal drugs and drug abuse
- i. Emotional and mental disorders
- j. Record of law violations
- k. Security violations

Adjudicative actions concerning the foregoing items are examined in greater detail below.

LOYALTY

DCID 1/14 establishes the categorical requirement that, to be eligible for SCI access, an individual must be of unquestioned loyalty to the United States.

CLOSE RELATIVES AND ASSOCIATES

DCID 1/14 requires close examination by the SCI adjudicator when members of an individual's immediate family and persons to whom he/she is bound by affection or obligation are not citizens of the United States, or their loyalty or affection is to a foreign power, or they are subject to any form of duress by a foreign power, or they advocate the violent overthrow or unconstitutional alteration of the Government of the United States.

The adjudicator must assess carefully the degree of actual and potential influence that such persons may exercise on the individual based on an examination of the frequency and nature of personal contact and correspondence with and the political sophistication and general maturity of the individual.

A recommendation for access disapproval is appropriate if there is an indication that such relatives or associates are connected with any foreign intelligence service.

When there is a "compelling need" for SCI access for an individual whose family member is a non-U.S. citizen and the background investigation indicates that the security risk is negligible, an exception to paragraph 5b(1), (2) of DCID 1/14 may be recommended.

In some circumstances, marriage of an individual holding SCI access approval could present an unacceptable security risk. An individual is required to file an intent to marry and it is the responsibility of the SIO to advise the individual of the possible security consequences. If the individual marries a non-U.S. citizen, SCI access will be suspended until the case is readjudicated unless an appropriate investigation of the spouse, as required by Paragraph 11L of DCID 1/14, was conducted with favorable results. In readjudicating such cases, the same judgments and criteria as reflected in this section apply.

HOMOSEXUAL CONDUCT AND SEXUAL PERVERSION

DCID 1/14 requires that, to be eligible for SCI access, individuals must be stable, of excellent character and discretion, and not subject to undue influence or duress through exploitable personal conduct.

Sexual conduct can be a relevant consideration in circumstances in which the conduct indicates a personality disorder or could result in exposing the individual to direct or indirect pressure because of susceptibility to blackmail or coercion as a result of the deviant sexual behavior. Such behavior includes: bestiality, fetishism, exhibitionism, necrophilia, nymphomania or satyriasis, masochism, sadism, pedophilia, transvestism, and voyeurism. Homosexual conduct is also to be considered as a factor in determining an individual's stability and susceptibility to undue influence or duress.

In examining cases involving acts of homosexual conduct or sexual perversion, it is relevant to consider the age of the person, the voluntariness, and the frequency of such activities, the public nature and the recency of the conduct, as well as any other circumstances which may serve to aggravate the nature or character of the conduct. A recommendation for disapproval is appropriate when, in view of all available evidence concerning the individual's history of sexual behavior, it appears that access to SCI could pose a risk to the national security.

COHABITATION

Extra-marital cohabitation with a member of the opposite sex, in and of itself, does not preclude SCI access approval.

The identity of a cohabitant must be ascertained and a determination made if such association constitutes an unacceptable security risk based on the same criteria as in the section dealing with Close Relatives and Associates. Cohabitation with an alien, for example, requires the same scrutiny as marriage to an alien. Extra-marital sexual relations are also of legitimate concern to the SCI adjudicator when the potential for undue influence or duress exists.

UNDESIRABLE CHARACTER TRAITS

It is emphasized that an individual's lifestyle is examined only in an effort to determine whether a pattern of behavior exists which indicates that granting SCI access could pose a risk to national security. In cases where allegations have been reported which reflect unfavorably on the reputation of an individual, it is incumbent upon the SCI adjudicator to distinguish fact from opinion and to determine which negative characteristics are real and pertinent to an evaluation of the individual's character and which are unsubstantiated or irrelevant. Relevant negative characteristics are those which, in the adjudicator's informed opinion, indicate that an individual is not willing, able, or likely to protect SCI information. The adjudicator's personal likes or dislikes must not be permitted to affect the determination.

Examples of specific concern in determining whether an individual has undesirable character traits are any substantive credible derogatory comments by associates, neighbors and other acquaintances; any litigation instituted against the individual by such persons as a result of the individual's actions; or allegations of violations of law. A recommendation for disapproval would be appropriate for an individual who cannot be relied upon to obey rules and regulations.

In examining the circumstances of cases involving incidents of untruthfulness, the adjudicator must weigh all factors with particular emphasis on establishing the intent of the individual. Where an individual has tried to obscure pertinent or significant facts by falsifying data, i.e. on the Personal History Statement by either omission or false entry, such action should be weighed heavily against recommending access. Failure to disclose derogatory personal information, such as a court martial or serious crime, would appear to be intentional and, consequently, would warrant a recommendation for disapproval.

FINANCIAL IRRESPONSIBILITY

Financial irresponsibility represents a serious concern to the SCI adjudicator. Persons who have engaged in espionage for monetary gain demonstrate the hazard of granting SCI access to an individual with overly expensive tastes and habits or living under the pressure of serious debt.

A recommendation for disapproval is appropriate when there is a pattern of financial irresponsibility and it appears that an individual has not made a conscientious effort to satisfy creditors. In such cases, the adjudicator should determine whether the individual had been notified about the debts and whether they were legally valid or ultimately satisfied.

When the financial irresponsibility alone is not of such magnitude to warrant disapproval, it may contribute to recommendation for denial of SCI access when there is other evidence of irresponsibility.

ALCOHOL ABUSE

The SCI adjudicator should examine any information developed relative to an individual's use of alcoholic beverages to determine the extent to which such use would adversely affect the ability of the individual to exercise the care, judgement, and discretion necessary to protect SCI information. The adjudicator should determine whether a pattern of impropriety exists, although one incident caused by alcohol abuse may be of such magnitude to warrant a recommendation for disapproval.

In determining the security impact of a person's pattern of alcohol use, the adjudicator should consider the circumstances, amount and rate of consumption, the time and place of consumption, and the physiological and behavioral effect such drinking has on the individual. For example, does the individual's drinking result in absences from work or careless work habits? Does the individual become talkative, abusive or manifest other undesirable characteristics? Does the individual drink until intoxicated? Has the individual been arrested for any acts resulting from the influence of alcohol?

In the absence of conclusive evidence, additional insight may be available from appropriate medical authorities. If the individual acknowledges having an alcohol abuse problem and is seeking help, it may be appropriate to defer access determination and monitor the individual's progress for a year or so.

If, after considering the nature and sources of the information, the adjudicator determines that an individual's drinking is not serious enough to warrant a recommendation for disapproval of SCI access, it may be appropriate to recommend approval with a warning at the time of indoctrination that future incidents of alcohol abuse may result in SCI denial. The adjudicator may also recommend a reinvestigation of the individual's use of alcohol after an appropriate period of time has passed.

ILLEGAL DRUGS AND DRUG ABUSE

The SCI adjudicator should examine all allegation of an individual's use, transport, transfer, sale, cultivation, processing and manufacturing of hallucinogens, narcotics, drugs and other materials and chemical compounds identified and listed in the Controlled Substance Act of 1970, as amended. Consequently an individual's involvement in any of these activities is of direct concern to the SCI adjudicator in order to determine the individual's capability to exercise the care, discretion, and judgement required to protect SCI information. The use of these substances may lead to varying degrees of physical or psychological dependence as well as having a deleterious effect on an individual's mental state and ability to function.

Persons involved in drug trafficking, i.e., the commercial cultivation, processing, manufacturing, purchase or sale of such substances should normally be recommended for disapproval.

In cases involving the use of drugs, the adjudicator must consider the nature of the substance used and whether the use is experimental or habitual. The frequency, recency and circumstances surrounding said use are key elements. For example, has the individual used "hard" drugs or hallucinogens such as heroin, cocaine or LSD? Has the individual used drugs regularly or only on occasion? Does the individual currently use drugs? Does the individual regularly purchase drugs or participate merely when offered drugs by others? Has the individual's behavior been affected by the use of drugs and, if so, to what extent?

Once the judgment is made that an individual is a habitual user of any controlled substance (multiple use beyond the point of mere experimentation), a recommendation for disapproval is appropriate. Moreover, even experimental use of hard drugs or hallucinogens, such as LSD, could warrant a recommendation for disapproval.

EMOTIONAL AND MENTAL DISORDERS

DCID 1/14 requires that persons considered for access to SCI be stable and of excellent character and discretion. Emotional and mental disorders which interfere with an individual's perception of reality or reliability are of serious concern to the SCI adjudicator in determining whether an individual is able or willing to protect SCI information.

It is essential to obtain as much information as possible when an allegation has been made in this area. If feasible, the individual should be interviewed to obtain additional details. When appropriate, government psychological and psychiatric personnel should be consulted so that psychiatric or psychological data may be properly evaluated.

If a current emotional instability appears to be a temporary condition, for example, caused by a death, illness or marital breakup, it may be advisable to recommend postponing final action and rechecking the situation at a later date. This precludes a security disapproval for what may be a temporary condition which, when cured, would have no security implications.

Military and civilian personnel who decline to take medical/psychiatric tests when so directed by competent authority should not be recommended for SCI access.

RECORD OF LAW VIOLATIONS

In determining whether an individual is stable, of excellent character and discretion as required by DCID 1/14 for access to SCI, the adjudicator must weigh carefully any record of law violations by the individual. Although a pattern of repeated minor traffic violations could be significant, the adjudicator is principally concerned with more serious criminal violations or court actions reflecting adversely upon the individual's reliability or trustworthiness.

Each case involving convictions for criminal offenses must be considered from the standpoint of the nature and seriousness of the offense, the circumstances under which it occurred, how long ago it occurred, whether it was an isolated offense or a repeated violation of the law, the offender's age at the time, social conditions which may have a bearing on the individual actions, and any evidence of rehabilitation.

Any conviction for a felony will normally support a recommendation for disapproval. If the offense was committed many years prior, the individual has shown evidence of rehabilitation, and the investigation shows no other derogatory information, an approval may be considered. A large number of minor offenses, however, could indicate irresponsibility and may support an adverse recommendation.

SECURITY VIOLATIONS

Most security violations are caused by carelessness or ignorance with no intention of compromising security. However, the record of an individual responsible for multiple violations should be scrutinized. The individual's current attitude toward security should be confirmed with his/her supervisor. A pattern of violations may be sufficient ground for a recommendation for disapproval.

ANNEX B

DCID 1/14 APPEALS PROCEDURES

USE OF THE POLYGRAPH IN SCREENING FOR SCI ACCESS

PROPOSED ANNEX C TO DCID 1/14

PURPOSE

1. Pursuant to the provisions of DCID 1/14, this Annex establishes minimum standards for use of the polygraph in screening individuals for initial or continued access to SCI. As the individual is one of the best sources of information regarding his own background, the polygraph examination clearly represents a productive adjunct to the security adjudication process. Complete, thorough, and detailed information cannot usually be obtained from a background investigation alone. Information derived from a polygraph interview provides important data to assist in proper adjudication for SCI access.

POLYGRAPH STANDARDS AND POLICIES

2. Each Intelligence Community organization shall establish and apply standards and policies governing the use of polygraph testing which shall pertain to, as a minimum, eligibility and physical fitness for testing, instrumentation utilized, training and certification of examiners, and supervision of polygraph results.

SCOPE OF POLYGRAPH TESTING

3. The polygraph examination shall be limited to topics essential to a security determination. For the purpose of this Annex, every polygraph examination shall include, as a minimum, the following topics:

- a. Subject identity.
- b. Involvement in or approaches to engage in espionage or sabotage on behalf of a foreign government.
- c. Clandestine or unreported meetings with representatives of a foreign government.
- d. Involvement in terrorism or subversion.

- e. Compromise or delivery of or approaches to divulge classified information to unauthorized persons.
- f. Knowledge of unreported incidents of compromise of classified information.
- g. Maintenance or storage of classified information outside of authorized areas.
- h. Removal of classified information without authorization.
- i. Involvement in bankruptcies, overburdening obligations, or concealed sources of income.
- j. Involvement in arrests, indictments, or convictions for any violation of law.
- k. Vulnerability to blackmail, coercion or duress.
- l. Any additional information necessary to resolve ambiguities developed by investigation.

USE OF POLYGRAPH RESULTS

4. The polygraph examiner shall not be involved in the access decision. Polygraph results will be submitted to an SCI access determination authority within each organization. That determination authority shall make the final access decision based upon information derived from the polygraph examination, the background investigation and other investigative efforts.

EFFECTIVE DATE

5. Interviews utilizing the polygraph will be required under the provisions of this directive beginning _____. Repolygraphing will be included as part of periodic reinvestigations beginning _____.

ANNEX D

**Minimum Standards For Security Awareness Programs
In The U.S. Intelligence Community**

Minimum standards are hereby established for the security education programs designed to enhance the security awareness of U.S. Government employees and private contractors working in the U.S. Intelligence Community. Compliance with these standards is required for all Departments/Agencies within the Intelligence Community. It is intended that existing security awareness programs shall be modified to conform with these standards. Departments/Agencies will establish a documented program, to ensure that training has been presented to all personnel.

The security awareness requirements set forth herein are divided into three phases. Phase I concerns the initial indoctrination of the employee which is normally administered prior to access to classified information. Phase II concerns the continuing security awareness program required to maintain and increase security awareness throughout the period of access. Phase III sets forth the final guidelines and instructions when access to classified information is terminated.

I. Initial Indoctrination—As soon as practicable after being approved for access to classified information, employees shall receive an initial security indoctrination which shall include:

A. The need for and purpose of classified information, and the adverse effects to the national security that could result from unauthorized disclosure.

B. The intelligence mission of the Department/Agency to include the reasons why intelligence information is sensitive.

C. The administrative, personnel, physical and other procedural security requirements of the Department/Agency, and those requirements peculiar to specific duty assignments.

D. Individual classification management responsibilities as set forth in appropriate directives and regulations to include classification/declassification guidelines and marking requirements.

E. The definitions and criminal penalties for espionage, including harboring or concealing persons;

gathering, transmitting, or losing defense information; gathering or delivering defense information to aid foreign governments; photographing and sketching defense installations; unauthorized disclosure of classified information (Title 18, U.S.C., Sections 792 through 795, 797 and 798), the Internal Security Act of 1950 (Title 50, U.S.C., Section 783) and, when appropriate, the Atomic Energy Act, Sections 224 through 227.

F. The administrative sanctions for violation or disregard of security procedures.

G. A review of the techniques employed by foreign intelligence organizations in attempting to obtain national security information.

H. Individual security responsibilities including:

1. The prohibition against discussing classified information in a nonsecure area, over a nonsecure telephone or in any other manner that permits access by unauthorized persons.

2. The need to determine, prior to disseminating classified information, that the prospective recipient has the proper security clearance, that the classified information is needed in order to perform official duties and that the recipient can properly protect the information.

3. Administrative reporting requirements such as foreign travel, contacts with foreign nationals, attempts by unauthorized individuals to obtain national security information, physical security deficiencies and loss or possible compromise of classified material.

4. Obligation to report to proper authorities any information which could reflect on the trustworthiness of an individual who has access to classified information, such as:

- a. Willful violation of security regulations
- b. Unexplained affluence or excessive indebtedness
- c. Serious unlawful acts

- d. Apparent mental or emotional problems
- e. Coercion or harassment attempts
- f. Blackmail attempts

5. Identification of the elements in the Department/Agency to which matters of security interest are to be referred.

II. Periodic Employee Awareness Enhancement—Each Department/Agency shall establish a continuing security awareness program which will provide for frequent exposure of personnel to viable security awareness material. Implementation of a continuing program may include live briefings, audio-visual presentations (e.g., video tapes, films and slide/tape programs), printed material (e.g., posters, memoranda, pamphlets, fliers) or a combination thereof. It is essential that current information and materials are utilized. Programs should be designed to meet the individual needs of the Department/Agency.

A. The basic elements for this program shall include, but are not limited to, the following:

- 1. The foreign intelligence threat.
- 2. The technical threat.
- 3. Administrative, personnel, physical and procedural security.
- 4. Individual classification management responsibility.
- 5. Criminal penalties and administrative sanctions.
- 6. Individual security responsibilities.
- 7. A review of other appropriate Department/Agency requirements.

B. Special security briefings/debriefings are required to supplement the existing security awareness programs in the following situations:

- 1. When an employee is designated as a courier.

2. When an employee travels, officially or unofficially, to or through communist countries, or areas of high risk.

3. When an employee has, or anticipates, contact with representatives of communist controlled countries.

4. When an employee is granted access to sensitive compartmented information or cryptographic material.

5. When any other situation arises for which a special briefing/debriefing is required by the Department/Agency.

III. Debriefing—When a Department/Agency has determined that access to classified information is no longer required, final instructions and guidelines will be provided to the employee. As a minimum these shall include:

A. A requirement that the individual read appropriate section of Titles 18 and 50, U.S. Code and that the intent and criminal sanctions of these laws relative to espionage and unauthorized disclosure be clarified.

B. The continuing obligation never to divulge, publish, or reveal by writing, word, conduct or otherwise, to any unauthorized persons any classified information relating to the national security, without the written consent of appropriate Department/Agency officials.

C. An acknowledgement that the individual will report without delay to the Federal Bureau of Investigation, or the Department/Agency, any attempt by an unauthorized person to solicit national security information.

D. A declaration that the individual no longer possesses any documents or material containing classified information.

E. A reminder of the risks associated with foreign travel and certain hazardous activities as defined in DCID 1/20, and Department/Agency reporting requirements as applicable.